# Healthcare

Customer case study

PHOENIX CONTACT
INSPIRING INNOVATIONS

## Major healthcare provider stays secure and virus-free with mGuard security devices


### Summary

- Devices and networks in the healthcare industry are becoming more interconnected, but FDA approvals and other industry issues can restrict patching and antivirus options
- This leaves the networks and data vulnerable to viruses and other breaches
- A major healthcare provider sought a dynamic and cost-effective solution that would mitigate threats and maintain acceptable security levels with the vendor-connected devices
- Phoenix Contact's mGuard SMART2 devices provided IT-approved security with easy-to-use features, such as USB power, remote configuration, simple cable management, and faster installation time


> "It is hard to quantify the impact of a security breach or virus. If we did not use this device, we would be vulnerable to both."
>
> **Security expert at healthcare company**

### Customer profile

In the healthcare industry, it is a continuing trend to connect diagnostic medical equipment with the corporate network for patient-data transfer to electronic medical records (EMR) and supporting systems. Within that realm, medical device manufacturers often produce equipment on standard operating systems, but due to FDA approval and functionality conflicts, vendors often restrict patching and antivirus options. This leaves the devices vulnerable if connected to a network. Other times, the devices themselves are on proprietary or closed platforms that don't offer any native firewall or security measures at all.

**Security is a concern in all industries, but in the healthcare market, FDA approvals and other industry issues can restrict patching and antivirus options.**

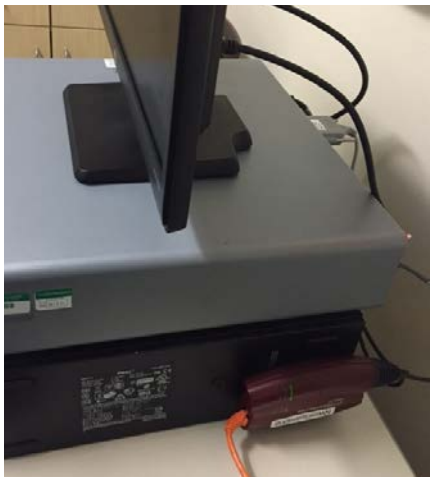
A major healthcare provider found that connecting these unprotected devices to its network greatly increased the risk of exposure – both for the medical device being networked and the corporate network itself. The company sought a dynamic and cost-effective solution that would mitigate threats but still maintain high security levels with the vendor-connected devices.

### Challenge: Connected medical networks risk exposure

The healthcare provider already had security devices in place, but these varied by location. In some select cases, the company used a security device with built-in firewall abilities. This legacy solution had an external power supply, making it cumbersome to manage. It was also a solution that was more complicated and

© 2017 PHOENIX CONTACT
003860A 11.17

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com



**Phoenix Contact's mGuard SMART2 devices provided IT-approved security with easy-to-use features, such as USB power, remote configuration, simple cable management, and faster installation time.**

potentially more confusing. Perhaps the biggest driver for the change was that this device had reached the end of its life span, and the manufacturer was no longer supporting it.

In other cases, the company connected medical devices to known ports being firewalled by another well-known IT brand. These security devices were expensive, especially due to the limited number of licenses that could be purchased for any given physical location.

Finally, some devices were connected to the network without any protection at all. This opened the gate to a potential security breach.

The healthcare company wanted to take a more formidable stance to protect the medical devices. Since it had to replace the obsolete hardware anyway, the security experts at the healthcare company wanted to find an economic solution that could be standardized, available anywhere, and centrally managed – all of which would protect the future of the company and its patients.

## Solution: Small but power security

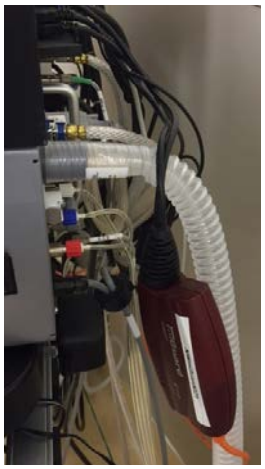
The healthcare provider selected Phoenix Contact's mGuard SMART2 security appliance. This small endpoint device features a powerful stateful-inspection firewall that is used to restrict ports and network traffic to just what is necessary for the data needs.

The mGuard offered several advantages over other security solutions on the market. It has a small form factor, clean cable management, and a high performance-to-cost ratio.

The mGuard SMART2 devices can also be powered via any USB port, which was very valuable for the healthcare provider. Over the past several years, mGuard devices have been installed in a variety of locations: exam rooms, screening rooms, and similar areas designed for patient care and medical data gathering where the medical equipment is located. Managing external AC power supplies in each of these diverse locations would be complicated, but the mGuard's convenient inline power supply eliminated the need for multiple external power supplies.

By applying the mGuard's preconfigured profiles, the healthcare company found it was quick and easy to deploy the mGuard. Basically, if an end user chooses a preconfigured device, he or she only has to plug it in – nothing else is needed.

The mGuard's central and remote management capabilities were also key benefits, allowing the security staff to manage multiple profiles remotely. When the company introduced a new server, causing connectivity issues, the staff used the remote management to quickly update the firewall rules, so that the mGuard can allow the diagnostic equipment to communicate with it. With assistance from Phoenix Contact security experts, the team developed enhanced feature requests and assistance with mGuard Device Management (MDM) installation.



**The healthcare provider has installed the mGuard SMART2 in a variety of locations: exam rooms, screening rooms, and similar areas designed for patient care and medical data gathering.**

Perhaps most importantly, the mGuard's high level of security met the corporate standards and gained approval from the enterprise IT department. This can be a daunting task at any large company, but in the highly regulated healthcare industry, it is even more critical.

## Results: Higher security and better peace of mind

The mGuard SMART2 is significantly less expensive than the IT-style solution the company previously used. In addition, the mGuards eliminated some of the secondary costs by not needing additional power or a complex management infrastructure to configure and administer them.

Since installing the mGuard devices several years ago, the security staff at the healthcare provider has been very pleased with the results. The diagnostic medical equipment has maintained uptime and been free from outside-influenced issues, such as viruses and malware. This not only keeps the devices themselves safe, but potentially the patient data as well.

A security expert at the company stated, "It is hard to quantify the impact of a security breach or virus. If we did not use this device, we would be vulnerable to both."

© 2017 PHOENIX CONTACT

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com